Foreign National Cyber Access
Risk Assessment
Version 1.5
February 6, 2002

Division :APS Number: FNCA-APS3
Prepared by: W. P. McDowell Date: September 26, 2002
Service/Computer/Cluster: APS Systems External Collaborators.

Instructions:

1. Use the form below to assess the vulnerabilities of your environment. Please extend the form if your environment has features not discussed below.
2. Identify the access controls you have in place to manage the user's environment. In addition to the standard login authentication processes, consider default file permissions, WWW content access, ftp server access, file sharing, etc. Provide enough detail to explain your answer.
3. Answering Yes or No to a question does not disqualify a legitimate user from accessing a computer system. Rather these questions are designed to help you assess the risks involved in granting any user access to a computer system by highlighting potential concerns.
4. You should only need one of these vulnerability assessments for each computing environment. Please update this form if your environment changes significantly.
5. Keep this on file in your division.

If this user will be provided a computer:

	Vulnerabilities	**Response/Access Controls**
1.	Are there data or applications on the computer that this user will be using that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	
2	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data on his computer? For example	
2.1	Have you removed the inappropriate data or applications?	
2.2	Are all users instructed in the secure management of data and applications?	
2.3	Does the computer system require authenticated access?	
2.4	Can you uniquely identify users?	
2.5	Do you establish minimal default file permissions for all accounts?	
2.6	How do you verify file permissions are correctly set for data and applications?	

If this user will be provided network access to computer services (mail, ftp, etc.):

	Vulnerabilities	**Response/Access Controls**
3.	Are there data or applications on the servers that this user will access that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	This computer is dedicated to software development. It contains no ANL Sensitive information.
4.	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data stored on computers providing these services? For example:	The default permissions for newly created files on this computer are 750 which provides access to only the user and his group members. Group members are allowed to only read and execute each other's files.

		The user must use SSH to initiate an interactive session to this computer. ftp and XWindows need to be tunneled through SSH.
4.1	Does having access to this server enable unauthenticated access to a local intranet (by virtue of having an *division.anl.gov* address)?	Yes. Access to this computer would enable the user to initiate a WWW browser and export the session back to their home computer. The user would have access to our divisional intranet. Division policy prevents sensitive material from appearing on our intranet WWW server. The user would also have access to the ANL intranet.
4.2	Does having an account on this server enable authenticated access to other computers?	No. As stated earlier, the accounts on this computer are not shared.
4.3	Are other computers sharing file systems that may be accessible from this server (e.g. NFS, Windows file shares)?	Yes.
4.3.1	If yes, how do you control network file access?	Users must login and are allowed access only to assigned development space.
4.3.2	How do you verify network file permissions are correct?	Scans and audits.

If this user's network connection provides intimate[1] access to a computing environment:

	Vulnerabilities	Response/Access Controls
5.	Are there data or applications in the network vicinity of this user's computer that are on the ANL Sensitive Technologies List or otherwise sensitive (privacy act, proprietary, OUO, etc.)?	Since access to this computer lets the user behind the Laboratory firewall, the user could see all Laboratory services a regular employee could see. Thus this user could electronically "touch" numerous computers with sensitive data unless those computer owners have taken steps to isolate them.
6.	Describe the mechanisms that will prevent this user from examining, altering, or using inappropriate applications or data stored on computers in the vicinity? For example (consider using nmap on the subnet to identify open services):	None. The other owners have the burden to protect their sensitive data from the general Laboratory population. This computer should, in general, not be trusted. Note the users of this computer are not granted administrator privilege and so would be unable use applications other than those standardly available to users.
6.1	Does having access to this computer enable unauthenticated access to a local intranet (by virtue of having an *division.anl.gov* address)?	Yes. See 4.1.

[1] For example: What is visible in the Network Neighborhood? Are there unrestricted NFS exports on the local network? If a user runs tcpdump or places an ethernet interface in promiscuous mode, what will they see?

6.2	Does having an account on this computer enable authenticated access to other computers?	No. See 4.2.
6.3	Are other computers sharing file systems that may be accessible to this computer (e.g. NFS, Windows file shares)?	Yes.
6.3.1	If yes, how do you control network file access?	Since users do not have administrator privilege they will not be able to vview these other shared file systems.
6.3.2	How do you verify network file permissions are correct?	Not applicable.